ОБ'ЄКТНО-ОРІЄНТОВАНИЙ ПІДХІД, ЯК ОСНОВА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Строков Є.М., ст. викладач кафедри економічного аналізу та обліку НТУ «ХПІ»

В сучасних умовах становлення та розвитку інформаційного суспільства невід'ємною часткою інфраструктури організації стають інформаційні системи, що забезпечують ефективне управління документообігом, персоналом, фінансами та виробництвом. Постійне зростання об'єму конфіденційної та критично важливої для підприємства інформації, що зберігається та обробляється у електронному вигляді потребує підвищення складності інформаційних систем. Використання інформаційних технологій з одного боку дає значні переваги, а з іншого – створює потенційні передумови до втрати, крадіжки, викривлення, підробки, знищення, копіювання або блокування інформації та, як слідство, нанесення економічного, соціального та інших видів збитку.

А, отже, одним з актуальніших та найважливіших питань, що постають перед підприємствами при забезпеченні ефективності функціонування, є його інформаційна безпека – оскільки порушення в цій сфері призводять до глибинних наслідків для будь-якого бізнесу.

Проблемам захисту інформаційних ресурсів підприємств та організацій присвячено роботи таких вчених як В.О. Галатенко [1, 2], Л.М. Кечиєва [3], А.А. Губенкова, В.Б. Байбуріна [4], С.Бармена [5], Л. Дж. Хофмана[6], Д.І. Стенга, С. Муна [7]. Крім того розроблено ряд міжнародних та національних стандартів, що регламентують питання інформаційної безпеки [8-12]. Проте питанням методичного забезпечення інформаційної безпеки приділяється недостатньо уваги.

Таким чином, постає питання визначення шляхів, що сприятимуть розробці ефективного методичного підходу до забезпечення захисту інформації в умовах розвитку інформаційної системи підприємства.

Під інформаційною безпекою слід розуміти захищеність інформації і підтримуючої інфраструктури від випадкових або навмисних впливів природного або штучного характеру, які можуть завдати неприйнятний збиток суб'єктам інформаційних відносин, у тому числі власникам і користувачам інформації і підтримуючої інфраструктури. В той час, як захист інформації – це комплекс заходів, спрямованих на забезпечення інформаційної безпеки.

Ключовими моментами в цьому визначенні є те, що інформаційна безпека залежить не тільки від комп'ютерів, але і від підтримуючої інфраструктури, до якої можна віднести системи електро-, водо-і теплопостачання, кондиціонери, засоби комунікацій і, обслуговуючий персонал, а також виділення поняття «неприйнятний збиток». Застрахуватись від усіх видів збитків неможливо, тим більше неможливо зробити це економічно доцільним способом, коли вартість захисних засобів і заходів не перевищує розмір очікуваного збитку. Значить, з чимось доводиться миритися і захищатися слід тільки від того, з чим змиритися ніяк не можна, тобто поріг неприйнятності має матеріальне вираження, а метою захисту інформації стає зменшення розмірів збитку до допустимих значень.

Виходячи з цих положень можна стверджувати, що інформаційна безпека не зводиться виключно до захисту від несанкціонованого доступу до інформації, це принципово ширше поняття та трактування проблем, пов'язаних з інформаційною безпекою, для різних категорій суб'єктів може істотно відрізнятися.

Таким чином, правильний з методологічної точки зору підхід до проблем інформаційної безпеки починається з виявлення суб'єктів інформаційних відносин та інтересів цих суб'єктів, пов'язаних з використанням інформаційних систем.

Під суб’єктами інформаційної безпеки слід розуміти:

- державу (в цілому або окремі її органи та організації);
- громадські або комерційні організації (об'єднання) і підприємства (юридичні особи);
- окремих громадян (фізичних осіб).

В процесі своєї діяльності суб'єкти можуть перебувати один з одним в різного роду відносинах: одержання, зберігання, обробка, розповсюдження та використання інформації.

Різні суб'єкти по відношенню до певної інформації можуть (можливо одночасно) виступати в якості:

- джерел або постачальників інформації;
- користувачів інформації;
- власників та/або розпорядників інформації;
- фізичних та юридичних осіб, про яких збирається або надається інформація;
- власників систем обробки інформації;
- учасників процесів обробки і передачі інформації і т.і.

Для успішного здійснення своєї діяльності суб'єкти інформаційних відносин зацікавлені в забезпеченні інформаційної безпеки, що характеризується наступними категоріями:

- конфіденційність – стан інформації, при якому доступ до неї здійснюють тільки суб'єкти, що мають на неї право;
- цілісність – уникнення несанкціонованої модифікації інформації;
- доступність – уникнення тимчасового або постійного приховування інформації від користувачів, що отримали права доступу.
- підзвітність – забезпечення ідентифікації суб'єкта доступу та реєстрації його дій;
- достовірність – відповідність передбаченій поведінці чи результату;

- автентичність або справжність –гарантія того, що суб'єкт або ресурс ідентичні заявленим.

В таких умовах системи інформаційної безпеки повинні вміти протистояти різноманітним атакам, як зовнішнім, так і внутрішнім, автоматизованим і скоординованим. Сучасна технологія програмування нажаль не дозволяє створювати безпомилкові програми, що не сприяє швидкому розвитку засобів забезпечення інформаційної безпеки. Слід виходити з того, що необхідно будувати надійні системи інформаційної безпеки із залученням ненадійних компонентів – програм.

В даний час інформаційна безпека є відносно замкнутої дисципліною, розвиток якої не завжди синхронізований із змінами в інших областях інформаційних технологій. Зокрема, в інформаційній безпеці поки не знайшли відображення основні положення об'єктно-орієнтованого підходу, що став основою при побудові сучасних інформаційних систем. Спроби створення великих систем ще в 60-х роках розкрили численні проблеми програмування, головною з яких є складність створюваних і супроводжуваних систем. Результатами досліджень у галузі технології програмування стали спочатку структуроване програмування, потім об'єктно-орієнтований підхід.

Об'єктно-орієнтований підхід є основою сучасної технології програмування, випробуваним методом боротьби зі складністю систем. Логічним і необхідним видається поширити цей підхід на системи інформаційної безпеки, для яких, як і для програмування в цілому, має місце згадана проблема складності.

Логічним є підхід боротьби зі складністю, що спирається на принцип розділення. У даному контексті цей принцип означає, що система інформаційної безпеки на вищому рівні повинна складатися з невеликої кількості відносно незалежних компонентів. Наступним кроком декомпозиції піддаються виділені компоненти, і так далі до заданого рівня деталізації. В

результаті система виявляється представленою у вигляді ієрархії з декількома рівнями абстракції.

Основна проблема структурного підходу, що застосовується зараз, полягає в тому, – непридатність на ранніх етапах аналізу і моделювання предметної області, коли до алгоритмів і функцій справа ще не дійшла.

Пропонуємий об'єктно-орієнтований підхід використовує об'єктну декомпозицію, тобто поведінка системи описується в термінах взаємодії об'єктів і не має такого концептуального розриву з аналізованими системами, і може застосовуватись на всіх етапах розробки і реалізації складних систем.

Проблема інформаційної безпеки – комплексна, багатогранна. Ці грані були визначені нами раніше: конфіденційність, цілісність, доступність, підзвітність, достовірність, автентичність. Їх можна досліджувати відносно незалежно, і вважається, що якщо всі вони забезпечені, то забезпечена і інформаційна безпека в цілому. Таким чином визначено цілі, і наступним етапом необхідно визначити засоби її досягнення.

Успіх в області інформаційної безпеки може принести тільки комплексний підхід. Тобто застосування заходів законодавчого, адміністративного, процедурного та програмно-технічного рівнів:

- законодавчі заходи забезпечення інформаційної безпеки (законодавчі та нормативно-правові акти);
- адміністративні заходи (накази керівництва організації, пов’язані із захистом інформаційних систем);
- процедурні заходи (заходи безпеки, що орієнтовані на персонал);
- програмно-технічні заходи.

Слід відзначити, що визначені грані можна розглядати також і як результат деталізації (законодавчий рівень, процес ний рівень і т.і.). Закони та нормативні акти орієнтовані на всіх суб'єктів інформаційних відносин незалежно від їх організаційної приналежності (це можуть бути як юридичні,

так і фізичні особи) в межах країни, адміністративні заходи – на всіх суб'єктів у межах організації, процедурні – на окремих людей (або невеликі категорії суб'єктів), програмно-технічні – на устаткування і програмне забезпечення. Такий підхід до трактування, в переході з рівня на рівень, дозволяє застосовувати спадкування (кожен наступний рівень не скасовує, а доповнює попередній) та поліморфізм (суб'єкти виступають відразу в декількох іпостасях – наприклад, як ініціатори адміністративних заходів і як звичайні користувачі, зобов'язані цим заходам підкорятися).

Зрозуміло, що виділені сукупності граней ортогональні, оскільки для певної грані однієї сукупності, грані в іншій сукупності повинні приймати всю множину можливих значень. Тобто для забезпечення достовірності інформації потрібно прийняти законодавчі, адміністративні, процедурні та програмно-технічні заходи.

Для наочності розглянемо застосування запропонованого підходу на прикладі інформаційної мережі умовної організації, що має підключення до Інтернет, для різних рівнів деталізації

Якщо розглядати інформаційну систему підприємства із нульовим рівнем деталізації, то бачимо лише, що на підприємстві є інформаційна система (рис. 1):

При розгляді на нульовому рівні ми бачимо лише, що підприємство має інформаційну систему. На цьому рівні необхідно враховувати законодавчі та нормативно-правові акти, що мають відношення до інформаційних систем та інформаційної безпеки. Можливо, що деяку інформацію неможна зберігати та/або обробляти на комп’ютерах, якщо інформаційна система не була відповідним чином атестована, або у підприємства не має дозволу (ліцензії) на таку діяльність. На рівні адміністрації декларуються цілі побудови інформаційної системи, правила закупівель, впровадження та експлуатації обладнання. Процедурний шар передбачає визначення вимог до фізичної

безпеки інформаційних систем. Програмно-технічні заходи на цьому рівні деталізації можуть визначати переважні апаратно-програмні платформи.

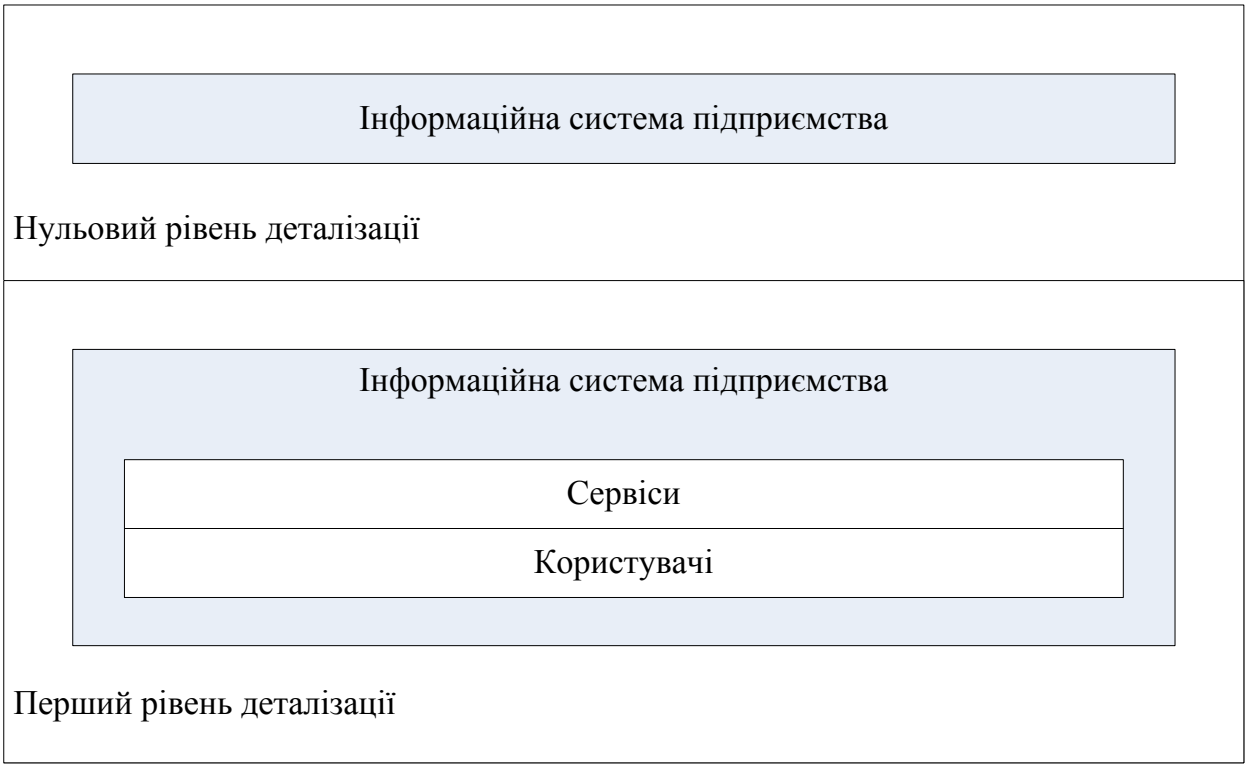

Рис. 10.1. Інформаційна система підприємства на нульовому та першому рівні деталізації

Перший рівень деталізації передбачає декомпозицію інформаційних систем до рівня сервісів та користувачів – розподілення на клієнтську та серверну частини. На цьому рівні формулюються вимоги до сервісів (їх наявність, доступність, цілісність, конфіденційність інформаційних послуг), засоби виконання цих вимог, визначення загальних правил поведінки користувачів, необхідного рівня їх підготовки, методи контролю. Можуть бути сформульовані вимоги до серверних та клієнтських платформ.

На другому рівні деталізації нас все ще не цікавить внутрішня структура інформаційної системи організації, так само як внутрішня структура мережі Інтернет та їх взаємозв'язок. Констатується лише наявність зв'язку між мережами, наявність користувачів та внутрішніх і надаваємих сервісів (рис. 10.2):

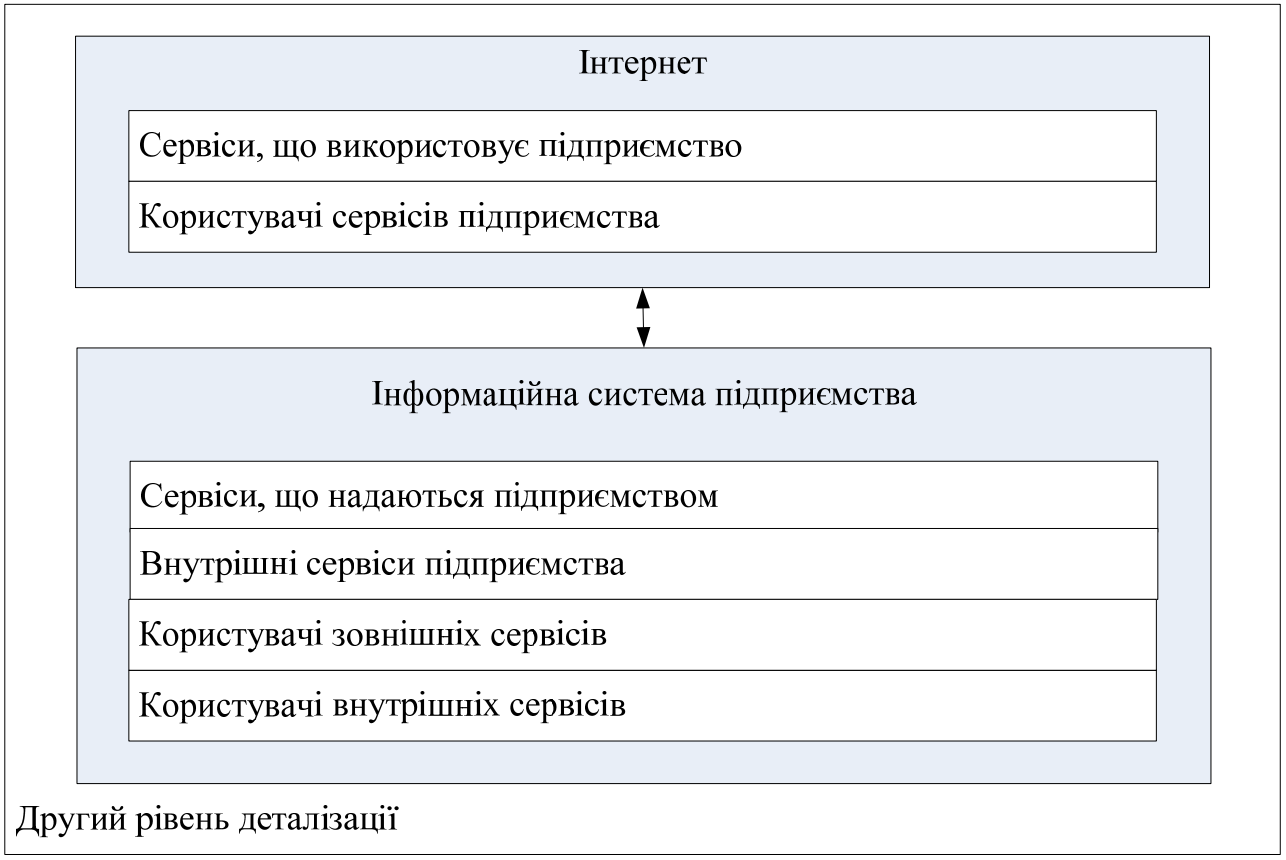

Рис. 10.2. Інформаційна система підприємства на другому рівні деталізації

На другому півні деталізації необхідно враховувати законодавчі акти, що застосовуються до організацій, інформаційні системи яких мають зовнішні підключення. Мова йде про допустимість такого підключення, його захисті, відповідальності користувачів, що мають доступ до зовнішніх сервісів, відповідальності організацій, що відкривають свої сервіси до зовнішнього

доступу. Аналогічна конкретизація виконується і на адміністративному, процедурному та програмно-технічному рівнях. Слід звернути увагу, що всі ці дії виконуються тільки в межі інформаційної системи підприємства, мережа Інтернет регулюється іншими правилами, які приймаються підприємством як даність.

Збільшення рівня деталізації дозволить дійти до категорій кінцевих користувачів, специфіки окремих сервісів, що вони використовують, зв'язків між ними, засобів забезпечення безпеки внутрішніх комунікацій і т.і.

Спираючись на вищезазначене можна стверджувати, що пропонуємий об'єктно-орієнтований підхід має майже необмежені можливості для деталізації та аналізу об'єктів інформаційної системи підприємства, і, як наслідок, забезпечує можливість побудови ефективної системи його інформаційної безпеки на всіх рівнях.

Список літератури: 1. *Галатенко В.А.* Основы информационной безопасности. – СПб. : Питер, 2006. – 204 с. **2.** *Галатенко В.А.* Стандарты информационной безопасности. – СПб. : Питер, 2006. – 236 с. **3.** *Кечиев Л.Н., Степанова П.В.* ЭМС и информационная безопасность в системах телекоммуникаций. – М. : Мысль, 2005. – 269 с. **4.** *Губенков А.А., Байбурин В.Б.* Информационная безопасность. – М. : Радио и связь, 2005. – 308 с. **5.** *Бармен С.* Разработка правил информационной безопасности. Пер. с англ. – М. : Издательский дом «Вильямс», 2002. – 208 с. **6.** *Л. Дж. Хофман* Современные методы защиты информации. Пер. с англ. – М.: Советское радио, 1980. – 264 с. **7.** *Стенг Д., Мун С.* Секреты безопасности сетей. – К. : «Диалектика», 1995. – 544 с. **8.** British Standard. Code of practice for information security management British Standards Institution, BS 7799:1995 **9.** British Standard. Information security management systems − Specification with guidance for use, British Standards Institution, BS 7799-2:2002. **10.** ГОСТ Р ИСО/МЭК 15408-2-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности. – Госстандарт России, Москва, 2002. **11.** ГОСТ Р ИСО/МЭК 15408-3-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности. – Госстандарт России, Москва, 2002. **12.** Common Criteria for Information Technology Security Evaluation. Version 2.2. Revision 256. Part 1: Introduction and general model. – January 2004.